PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-271312
(43)Date of publication of application : 20.09.2002

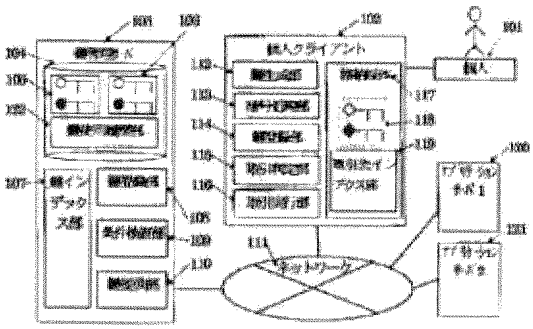
(51)Int.Cl. H04L 9/08
H04L 9/32

(21)Application number : 2001-071581
(22)Date of filing : 14.03.2001

(71)Applicant : HITACHI LTD
(72)Inventor : NINOMIYA TOSHIHIKO
MATSUNAGA KAZUO

(54) DISCLOSED KEY MANAGING METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To reduce the load on key management in the case that an individual manages disclosed key pairs for every application server providing service, in the service in which verification for defining the other party of electronic commercial trade using a network is necessary, security must be ensured, and capacity necessary for an individual terminal cannot be increased when the number of application servers performing trade is increased.
SOLUTION: The paired disclosed keys for trade allocated to every application server are not held and managed by an individual but are registered in a key managing server, thereby making individual key management unnecessary. The paired disclosed keys to be registered are enciphered by using a managing key of the individual, thereby ensuring security. Various additional information is registered together with the keys registered in the management server, thereby enabling much additional service. The load on individual key management is reduced, and the capacity of an individual terminal is not increased when the number of application servers of customers are increased. In this case, security of the key for trade can be ensured, and various kinds of service added to key management can be executed to all the individuals.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－271312
（P2002－271312A）
(43)公開日　平成14年９月20日(2002.9.20)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ａ	５Ｊ１０４
9/32			６０１Ｆ	
			６７５Ｂ	

審査請求　未請求　請求項の数７　ＯＬ　（全 11 頁）

(21)出願番号　特願2001－71581(P2001－71581)

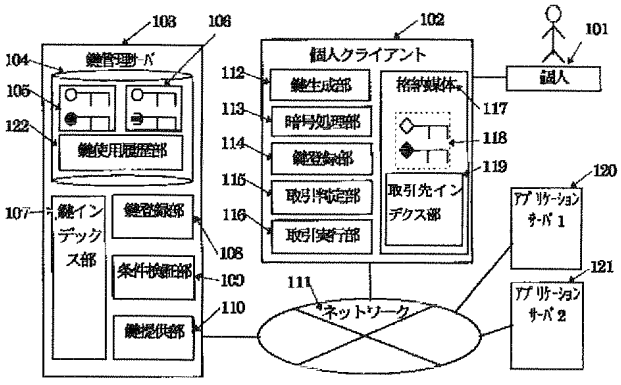
(22)出願日　平成13年３月14日(2001.3.14)

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　二宮　敏彦
神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウェア事業部内
(72)発明者　松永　和男
神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウェア事業部内
(74)代理人　100096954
弁理士　矢島　保夫

Ｆターム(参考)　5J104 AA16 EA01 EA04 EA17 NA02 PA07

(54)【発明の名称】　公開鍵管理方法

(57)【要約】
【課題】ネットワークを利用して電子商取引等の相手を特定するための認証が必要になるサービスにおいて、サービスを提供するアプリケーションサーバ毎に、個人が取引用公開鍵ペアを管理するような場合の鍵管理の負担を軽減する。この際、セキュリティも確保しておく必要がある。また取引を行うアプリケーションサーバの数が増えても、個人の端末に必要な容量は増せない。
【解決手段】アプリケーションサーバ毎の取引用公開鍵ペアを個人が保持・管理せずに、鍵管理サーバに登録することにより、個人の鍵管理を不要にする。また登録する取引用公開鍵ペアは、個人の鍵管理用鍵で暗号化することにより、セキュリティを確保する。鍵管理サーバに登録する鍵と共にいろいろな付加情報を登録することにより、多くの付加サービスが可能となる。
【効果】個人の鍵管理の負荷が軽減する。また取引先のアプリケーションサーバが増えても、個人端末の容量は増えない。このときの取引用鍵のセキュリティも確保できる。また鍵管理に付加するいろいろなサービスがすべての個人に実施できる。



【特許請求の範囲】
【請求項１】クライアントからネットワーク経由でアプリケーションサーバに接続し各種の取引を行う際に使用する前記クライアントの公開鍵を管理する公開鍵管理方法であって、
前記クライアントは、該クライアントで作成した前記アプリケーションサーバごとの取引用公開鍵ペアを暗号化するための管理用の暗号鍵を保持し、
前記ネットワークには、前記管理用の暗号鍵により暗号化された前記クライアントの取引用公開鍵ペアを格納するための鍵管理サーバを設置することを特徴とする公開鍵管理方法。
【請求項２】クライアントからネットワーク経由でアプリケーションサーバに接続し各種の取引を行う際に使用する前記クライアントの公開鍵を管理する公開鍵管理方法であって、
前記クライアントで、前記アプリケーションサーバごとの取引用公開鍵ペアを暗号化するための管理用の暗号鍵を作成し、保持するステップと、
前記クライアントで、前記アプリケーションサーバごとに取引用公開鍵ペアを生成するステップと、
前記クライアントで、前記生成した取引用公開鍵ペアを前記管理用暗号鍵で暗号化するステップと、
前記暗号化された取引用公開鍵ペアを、前記ネットワークに接続された鍵管理サーバに送信するステップと、
前記鍵管理サーバで受信した前記暗号化された取引用公開鍵ペアを所定の記憶手段に格納するステップと、
前記クライアントから前記アプリケーションサーバに接続して取引きするため、前記鍵管理サーバから前記暗号化された取引用公開鍵ペアを取得するステップと、
取得した取引用公開鍵ペアを、前記保持してある管理用暗号鍵で復号するステップと、
復号した取引用公開鍵ペアを用いて前記アプリケーションサーバとの取引きを実行するステップとを備えたことを特徴とする公開鍵管理方法。
【請求項３】請求項１または２に記載の公開鍵管理方法において、
前記鍵管理サーバで、前記取引用公開鍵ペアの有効期限を管理し、該有効期限が満了したとき、または、該有効期限満了前の所定期間に至ったときに、前記クライアントに対して取引用公開鍵ペアの更新を行うべきことを通知するステップを、さらに備えたことを特徴とする公開鍵管理方法。
【請求項４】請求項１または２に記載の公開鍵管理方法において、
前記鍵管理サーバで、前記取引用公開鍵ペアの使用回数、最終使用の日時、または使用履歴を管理し、これらの情報に基づいて不正な使用を検出するステップを、さらに備えたことを特徴とする公開鍵管理方法。
【請求項５】請求項４に記載の公開鍵管理方法において、
不正な使用を検出したとき、前記取引用公開鍵ペアの使用を制限または禁止するステップを、さらに備えたことを特徴とする公開鍵管理方法。
【請求項６】請求項１または２に記載の公開鍵管理方法において、
前記鍵管理サーバに格納する前記取引用公開鍵ペアのうち、公開鍵は平文で格納することを特徴とする公開鍵管理方法。
【請求項７】請求項１、２、または６に記載の公開鍵管理方法において、
前記鍵管理サーバに前記クライアントの鍵管理用公開鍵をさらに保管し、前記取引用公開鍵ペアの使用時に、前記鍵管理用公開鍵を用いて個人認証を実施することを特徴とする公開鍵管理方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ネットワークを利用して電子商取引などを行う際に使用する鍵管理技術に関する。
【０００２】
【従来の技術】ネットワークを利用して電子商取引などを行う場合、相手を特定するための認証処理が必要である。認証処理には鍵（証明書）を利用するが、通常は、サービスを提供するアプリケーションサーバ毎に、個人が例えば取引用公開鍵ペア（公開鍵暗号技術により生成される公開鍵と秘密鍵のペア）を生成し、自分自身で管理して使い分けていた。したがって、例えばクレジットカード決済や銀行決済においては、取り引きするクレジットカード会社や銀行毎に、個人は別々の取引用公開鍵ペアを管理する必要があった。
【０００３】また、ＳＥＴ（Visa InternationalとMasterCard Internationalの策定したSecure Transaction Protocol）の推進団体であるＳＥＴＣｏに提案されている"Server-Based Wallet Security Proposal"に示されているようにＷａｌｌｅｔ（消費者が使用する電子決済ソフトウェア）機能をサーバ側で実行し、個人クライアントからはＷｅｂブラウザでサーバ経由で電子商店などのアプリケーションサーバにアクセスする方法など、個人の鍵管理を代行するサーバを設置する方式があるが、これは代行するサーバでアプリケーションを実行してアプリケーションサーバと個人の接続を中継する方式である。
【０００４】特開２０００－４９７６６には、各個人がアプリケーションサーバ毎に鍵管理を行う負担を軽減するため、鍵管理サーバを設け、該鍵管理が鍵生成とアプリケーション用公開鍵証明書の取得を自動的に行う技術が開示されている。
【０００５】
【発明が解決しようとする課題】上述したように、各個

人は、電子商取引などのサービスを提供するアプリケーションサーバ毎に鍵管理を行わなければならず管理の負担が少なくなかった。

【０００６】また、各個人で複数の取引用公開鍵ペアを保持する場合、それらの鍵を記憶しておく記憶手段に大きな容量が必要であるため、携帯端末からの取引が不可能である場合があった。

【０００７】上述の鍵管理をサーバで代行する技術によれば、アプリケーションサーバ毎の個人側のアプリケーション実行をサーバで代行するので、代行するサーバの負荷が大きい。また代行するサーバが個人の公開鍵ペアを管理するためセキュリティ上の問題があり、さらに高度のセキュリティを実現するためには代行するサーバの負担が非常に大きいという問題がある。

【０００８】さらに、特開２０００－４９７６６の技術では、取引用公開鍵ペアを作成・管理するのは鍵管理サーバであるため、セキュリティ上の問題がある。

【０００９】本発明は、サービスを提供するアプリケーションサーバ毎に鍵管理が必要な場合でも、各個人の鍵管理の負担を軽減し、かつ携帯端末からの取引も容易で、セキュリティも確保することができるような鍵管理方法を提供することを目的とする。

【００１０】

【課題を解決するための手段】上記目的を達成するため、本発明は、クライアントからネットワーク経由でアプリケーションサーバに接続し各種の取引を行う際に使用する前記クライアントの公開鍵を管理する公開鍵管理方法であって、前記クライアントは、該クライアントで作成した前記アプリケーションサーバごとの取引用公開鍵ペアを暗号化するための管理用の暗号鍵を保持し、前記ネットワークには、前記管理用の暗号鍵により暗号化された前記クライアントの取引用公開鍵ペアを格納するための鍵管理サーバを設置することを特徴とする。

【００１１】また本発明は、クライアントからネットワーク経由でアプリケーションサーバに接続し各種の取引を行う際に使用する前記クライアントの公開鍵を管理する公開鍵管理方法であって、前記クライアントで、前記アプリケーションサーバごとの取引用公開鍵ペアを暗号化するための管理用の暗号鍵を作成し、保持するステップと、前記クライアントで、前記アプリケーションサーバごとに取引用公開鍵ペアを生成するステップと、前記クライアントで、前記生成した取引用公開鍵ペアを前記管理用暗号鍵で暗号化するステップと、前記暗号化された取引用公開鍵ペアを、前記ネットワークに接続された鍵管理サーバに送信するステップと、前記鍵管理サーバで受信した前記暗号化された取引用公開鍵ペアを所定の記憶手段に格納するステップと、前記クライアントから前記アプリケーションサーバに接続して取引きするため、前記鍵管理サーバから前記暗号化された取引用公開鍵ペアを取得するステップと、取得した取引用公開鍵ペアを、前記保持してある管理用暗号鍵で復号するステップと、復号した取引用公開鍵ペアを用いて前記アプリケーションサーバとの取引きを実行するステップとを備えたことを特徴とする。

【００１２】また本発明は、上述の公開鍵管理方法において、前記鍵管理サーバで、前記取引用公開鍵ペアの有効期限を管理し、該有効期限が満了したとき、または、該有効期限満了前の所定期間に至ったときに、前記クライアントに対して取引用公開鍵ペアの更新を行うべきことを通知するステップを、さらに備えたことを特徴とする。

【００１３】また本発明は、上述の公開鍵管理方法において、前記鍵管理サーバで、前記取引用公開鍵ペアの使用回数、最終使用の日時、または使用履歴を管理し、これらの情報に基づいて不正な使用を検出するステップを、さらに備えたことを特徴とする。

【００１４】また本発明は、上述の公開鍵管理方法において、不正な使用を検出したとき、前記取引用公開鍵ペアの使用を制限または禁止するステップを、さらに備えたことを特徴とする。

【００１５】また本発明は、上述の公開鍵管理方法において、前記鍵管理サーバに格納する前記取引用公開鍵ペアのうち、公開鍵は平文で格納することを特徴とする。

【００１６】さらに本発明は、上述の公開鍵管理方法において、前記鍵管理サーバに前記クライアントの鍵管理用公開鍵をさらに保管し、前記取引用公開鍵ペアの使用時に、前記鍵管理用公開鍵を用いて個人認証を実施することを特徴とする。

【００１７】上記構成により、各クライアントはサービスを利用するアプリケーションサーバ毎に取引用公開鍵ペアを生成するが、生成した取引用公開鍵ペアは各クライアントが保持・管理するのでなく、鍵管理サーバに登録することにより、各クライアントでの鍵管理が不要となる。また、登録する各クライアントの公開鍵ペアは、個人の管理用暗号鍵（共通鍵または公開鍵ペア）により暗号化して登録することにより、他者に個人の取引用公開鍵ペアを知られることを防ぐことができる。また、鍵管理サーバに登録する際に、各クライアント対応のインデクス及びアプリケーションサーバ対応のインデクスで管理することで、個人が取引時に、取引用公開鍵ペアを鍵管理サーバから取得する際に必要な鍵を特定する。さらに、鍵情報には有効期限、使用回数限度、使用回数、及び最終使用日時を同時に記録しておき、使用条件の検証を行うことにより、不正な使用を検出することができる。

【００１８】

【発明の実施の形態】以下、本発明の実施の形態を図面により詳細に説明する。

【００１９】図１は、本発明の第１の実施形態に係るシステムの構成図で、取引先インデクスを個人クライアン

トの中に持つ場合の構成である。個人クライアント１０２、鍵管理サーバ１０３、アプリケーションサーバ１（１２０）、及びアプリケーションサーバ２（１２１）が、ネットワーク１１１で接続されている。

【００２０】個人クライアント１０２は、個人１０１が使用するもので、鍵生成部１１２、暗号処理部１１３、鍵登録部１１４、取引判定部１１５、取引実行部１１６、及び格納媒体１１７を備えている。鍵生成部１１２は、個人の鍵管理用鍵１１８や取引用公開鍵ペア１０５，１０６を生成する。暗号処理部１１３は、鍵生成部１１２で生成した取引用公開鍵ペア１０５，１０６を鍵管理用鍵１１８で暗号化したり、鍵管理サーバ１０３から取得した暗号化された取引用公開鍵ペア１０５，１０６を復号する。鍵登録部１１４は、暗号化された取引用公開鍵ペア１０５，１０６を鍵管理サーバ１０３に登録する。

【００２１】取引判定部１１５は、取引用公開鍵ペア１０５，１０６の有効期限や使用回数等の使用条件の報告を鍵管理サーバ１０３から受け、取引を実施するか判定する。取引実行部１１６は、取引判定部１１５の判定で取引を行う場合、鍵管理サーバ１０３から取得し暗号処理部１１３で復号化された取引用公開鍵ペア１０５，１０６を使用して、アプリケーションサーバ１（１２０）やアプリケーションサーバ２（１２１）と取引きを実施する。格納媒体１１７には、鍵管理用鍵１１８、及び取引用公開鍵ペアがどのアプリケーションサーバと対応したものかを示す取引先インデクス１１９が、格納される。

【００２２】鍵管理サーバ１０３は、鍵格納部１０４、鍵インデクス部１０７、鍵登録部１０８、条件検証部１０９、及び鍵提供部１１０を備える。鍵格納部１０４は、個人クライアント１０２から登録依頼をうけた取引用公開鍵ペア１０５，１０６（個人の鍵管理用鍵１１８で暗号化されている）を格納する部位である。また鍵使用の履歴１２２も格納している。鍵インデクス部１０７は、登録した鍵、個人、及び取引先の関連付けを示すインデクスで、図１５（後述）にその内容を示している。鍵登録部１０８は、個人クライアント１０２から依頼された取引用公開鍵を鍵格納部１０４に登録し、鍵インデクス部１０７を更新する。条件検証部１０９は、取引用公開鍵１０５，１０６の有効期限や使用回数限度などを検証し、期限や限度等が超過していれば、個人クライアント１０２に連絡する。鍵提供部１１０は、個人クライアント１０２からの要求により鍵格納部１０４に登録されている取引用公開鍵ペアを個人クライアント１０２に送信する。

【００２３】なお、図１の鍵管理用鍵１１８は、秘密鍵と公開鍵のペアからなるように図示しているが、これに限らず、単一の共通鍵を用いてもよい。後述する図２及び図３のシステムの鍵管理用鍵２１８，３１８も同様である。

【００２４】図２は、本発明の第２の実施形態に係るシステムの構成図で、取引先インデクスを鍵管理サーバの中に持つ場合の構成である。図１では個人クライアント１０２の格納媒体１１７にあった取引先インデクス部１１９が、図２では鍵管理サーバ２０３の中に設けてある。取引先インデクス２１９は、図１では個人毎にばらばらに存在し、取引先ＩＤもばらばらだった取引先インデクスが、鍵管理サーバ２０３で１個に統一され、同じアプリケーションサーバであれば、同じ取引先ＩＤを持つことになり、管理し易くなる。なお、図２の２００番台の構成要素と図１の１００番台の構成要素とは、下２桁が同じ番号の構成要素同士が対応しているものとする。

【００２５】図３は、本発明の第３の実施形態に係るシステムの構成図で、鍵管理サーバに登録した取引用公開鍵ペアのうち公開鍵は暗号化せずに登録する場合の構成である。図２と比べて、鍵管理サーバ３０３に公開鍵認証部３２２が追加される。取引用公開鍵ペアのうち公開鍵は暗号化していないので、個人３０１またはアプリケーションサーバ３２０，３２１から個人３０１の取引用公開鍵について検証依頼があった場合、個人３０１に問い合わせず、鍵管理サーバ３０３で認証が可能となる。なお、図３の３００番台の構成要素と図２の２００番台の構成要素とは、下２桁が同じ番号の構成要素同士が対応しているものとする。

【００２６】図４は、本発明の第４の実施形態に係るシステムの構成図で、個人の鍵管理用公開鍵ペアの公開鍵を暗号化せず鍵管理サーバに登録する場合の構成である。図１～３のシステムでは鍵管理用鍵１１８，２１８，３１８は公開鍵ペアでも共通鍵でもよかったが、図４では、個人クライアント４０２の格納媒体４１７に格納されている鍵管理用鍵４１８は公開鍵ペアである。また鍵管理サーバ４０３には個人認証部４２６が追加され、鍵格納部４０４には鍵管理用鍵４１８の公開鍵である鍵管理用公開鍵４２３が登録されている。個人認証部４２６は、個人クライアント４０２からの鍵管理用鍵４１８の秘密鍵で署名された個人証明書を受け取り、鍵管理用公開鍵４２３で検証する。

【００２７】以下、フローチャートを用いて、上述の実施形態のシステムの動作を説明する。

【００２８】図５は、図１のシステムにおける個人の管理用鍵１１８の生成のフローチャートを示したものである。個人クライアント１０２において個人の管理用鍵１１８の生成の開始が指示されると（ステップ５０１）、図１の個人クライアント１０２の鍵生成部１１２において、暗号鍵を生成する（ステップ５０２）。暗号技術としては、公開鍵暗号技術として既に公知となっているＲＳＡ暗号や楕円曲線暗号技術などを利用することができる。また共通鍵暗号の技術も適用可能である。生成した

暗号鍵１１８は格納媒体１１７に格納する（ステップ５０３）。ここでは図１のシステムにおける管理用鍵生成の流れを説明したが、図２、及び図３のシステムでも同じである。図４のシステムにおける個人の管理用鍵の生成と登録の流れは、図１２で後述する。

【００２９】図６は、図１のシステムにおける取引用鍵１０５，１０６の生成と登録のフローチャートを示したものである。個人クライアント１０２において取引用鍵の生成と登録の開始が指示されると（ステップ６０１）、図１の個人クライアント１０２の鍵生成部１１２で取引用の公開鍵ペアを生成する（ステップ６０２）。次に、この公開鍵ペアを使用するアプリケーションサーバが格納媒体１１７に格納されている取引先インデクス部１１９に登録されているか否か検索し（ステップ６０３）、登録されていなければ新規取引先として取引先インデクス部１１９に追加する（ステップ６０４）。

【００３０】次に、取引先インデクス番号（取引先ＩＤ）を取得する（ステップ６０５）。ステップ６０２で生成した取引用公開鍵ペアを、格納媒体１１７に格納されている管理用鍵１１８で、暗号化する（ステップ６０６）。この暗号化した取引用公開鍵ペアと個人ＩＤ、取引先ＩＤ、及び鍵の有効期限や使用回数限度などの使用条件を管理サーバ１０３に送信し鍵格納部１０４に登録する（ステップ６０７）。なお、図２～図４のシステムにおける取引用鍵の生成と登録の流れは、図１０を参照して後述する。

【００３１】図７は、図１のシステムにおける取引の実行のフローチャートを示したものである。個人クライアント１０２において取引の実行の開始が指示されると（ステップ７０１）、まず個人クライアント１０２の格納媒体１１７に格納されている取引先インデクス部１１９を検索して使用するアプリケーションサーバの取引先インデクス番号（取引先ＩＤ）を取得する（ステップ７０２）。例えば図１６の取引先インデクスでは、「Ａ銀行との取引であれば、取引先ＩＤは００１」というように個人１０１が取引毎に特定することができる。次に鍵管理サーバ１０３に個人ＩＤと取引先ＩＤを送信して取引用公開鍵ペアの取得を要求する（ステップ７０３）。取得した取引用公開鍵ペアは暗号化されているため、個人管理用鍵１１８を使用して復号化する（ステップ７０４）。復号化された取引用公開鍵を使用して、アプリケーションサーバと取引を実行する（ステップ７０６）。

【００３２】ここでの取引の実行は公知の公開鍵暗号技術を使用した取引で、例えばVisa InternationalとMasterCard Internationalの策定したＳＥＴ(Secure Transaction Protocol)のような取引方式が利用できる。

【００３３】なお、ここでは図１のシステムにおける取引実行の流れを説明したが、図２及び図３のシステムでも同様である。ただし、図２及び図３のシステムでは取引先インデクス部が鍵管理サーバ内に設けられているので、ステップ７０２の処理では鍵管理サーバの取引先インデクスを検索することになる。あるいは、鍵管理サーバに取引先名称などの取引先インデクスを検索するキーとなる情報を渡し、鍵管理サーバ側で取引先ＩＤを求めて取引用公開鍵ペアの検索に利用してもよい。図４のシステムにおける取引実行の流れは、図１３で後述する。

【００３４】図８は、図１のシステムにおける鍵管理サーバ１０３の条件検証部１０９で、有効期限のチェックと満了の通知をする場合のフローチャートを示したものである。鍵管理サーバ１０３における条件検証（有効期限の通知）の処理（ステップ８０１）では、個人クライアント１０２からの取引用公開鍵ペア登録依頼の際、同時に送信される鍵の有効期限を図１５に示す鍵インデクス１０７に登録する（ステップ８０２）。

【００３５】その後、所定時間間隔でタイマー通知のプロセス（ステップ８０４）を繰り返し実行する。このタイマー通知では、鍵インデクス部１０７に登録されているすべての取引用公開鍵ペアの有効期限をチェックし（ステップ８０５）、有効期限を超過している取引用公開鍵ペアがあれば、その所有者である個人クライアントに有効期限満了を通知する（ステップ８０６）。これにより、個人１０１は個人取引用鍵の有効期限満了を随時意識する必要が無く、通知を受けた時点で取引用公開鍵の生成(更新)を実行することで継続して有効な公開鍵を維持することができる。

【００３６】ここでは図１のシステムにおける条件検証処理の流れを説明したが、図２～図４のシステムでも同様である。また、ここでは有効期限が満了したときに通知しているが、有効期限の満了前の所定期間に至ったときに通知するようにしてもよい。

【００３７】図９は、図１のシステムにおける鍵管理サーバ１０３の条件検証部１０９で、使用回数のチェックとその限度超過の通知をする場合のフローチャートを示したものである。予め、個人クライアント１０２からの取引用公開鍵ペア登録依頼の際、同時に送信される鍵の使用回数限度を図１５に示す鍵インデクス１０７に登録しておく。図１５のように、累積使用回数限度１５１０、１日使用回数限度１５１１、１週間使用回数限度１５１２、及び１月使用回数限度１５１３を登録すれば、時間単位の管理が可能である。状況により別の時間単位にすることも可能である。

【００３８】図９の鍵管理サーバ１０３での条件検証（使用回数限度の通知）処理は、個人クライアントから取引用公開鍵ペアの送付要求が来た場合に起動する。本処理が開始すると（ステップ９０１）、取引用公開鍵ペアの使用、すなわち取引用公開鍵ペアを個人クライアントに送付し（ステップ９０２）、その鍵の使用回数１５０５～１５０７を＋１更新（カウントアップ）する（ステップ９０３）。このとき、現在時点が、１日、１週間、あるいは１月の使用回数をカウントする時間区間の

区切りに至っていたときは、その使用回数のカウンタ１５０５～１５０７をゼロクリアした後、カウントアップするものとする。次に、それぞれの時間単位（１日、１週間、１月）の使用回数限度をチェックし（ステップ９０４）、超過していれば当該取引用公開鍵ペアの所有者の個人クライアントに使用回数限度超過を連絡する（ステップ９０５）。この際、使用回数、最終使用時刻、及び使用履歴も要求により送付する。

【００３９】個人１０１は、この使用回数限度超過の通知を受信すると、自分自身で記録している使用回数、最終使用時刻、及び使用履歴と比較し、不正使用の有無を判定する。不正使用と判定した場合は、鍵管理サーバ１０３に登録してある取引用鍵の変更、鍵管理サーバ１０３のパスワード等の認証情報の変更が必要である。また使用回数限度超過報告（ステップ９０５）が送信される場合だけでなく、必要な場合に鍵管理サーバ１０３に問合わせし、使用回数、最終使用時刻、及び使用履歴等の使用状況情報を取得して、個人１０１がその都度不正使用を判定することも可能である。

【００４０】ここでは図１のシステムにおける条件検証処理の流れを説明したが、図２～図４のシステムでも同様である。

【００４１】図１０は、図３のシステムにおける取引用鍵３０５，３０６の生成と登録の流れ、すなわち取引先インデクス部３１９を鍵管理サーバ３０３に持ち取引用鍵のうち秘密鍵のみ暗号化する場合のフローチャートを示したものである。ステップ１００２，１００３は図６のステップ６０２，６０３と、ステップ１００４～１００８は図６のステップ６０３～６０７と、同様の処理である。図６との相違は、取引先インデクスを検索する場合、個人クライアントの取引先インデクスでなく、鍵管理サーバ３０３の取引先インデクス３１９を検索し（ステップ１００３）、取引用公開鍵ペア３０５，３０６の暗号化は秘密鍵のみを個人管理用鍵３１８で暗号化することである（ステップ１００７）。

【００４２】取引先インデクス部３１９が鍵管理サーバ３０３にあることにより、サーバ側で取引先毎の管理が容易になる。なお、ここでは図３のシステムにおける取引用鍵の生成と登録の流れを説明したが、図２及び図４のシステムでも同様である。ただし、図２のシステムでは取引用公開鍵ペア２０５，２０６は秘密鍵と公開鍵の両方を個人管理用鍵２１８で暗号化するためステップ１００７では秘密鍵だけでなく公開鍵も暗号化する。

【００４３】図１１は、図３のシステムにおいて図１０で暗号化せずに登録した取引用公開鍵ペア３０５，３０６の公開鍵の認証を鍵管理サーバ３０３で行う場合のフローチャートを示したものである。ここではアプリケーションサーバ１（３２０）から個人３０１の取引用公開鍵の検証を依頼された場合について説明する。取引用公開鍵の認証が開始されると（ステップ１１０１）、検証を依頼されたアプリケーションサーバ１（３２０）から取引用公開鍵の検証依頼を受け付け（ステップ１１０２）、取引先インデクス３１９からアプリケーションサーバ１（３２０）と個人ＩＤの該当する取引用公開鍵ペアを検索し、その公開鍵を見つけ出す（ステップ１１０３）、この公開鍵とアプリケーションサーバ１（３２０）から送付された公開鍵とを比較し（ステップ１１０４）、一致すれば認証したことをアプリケーションサーバ１（３２０）に連絡する（ステップ１１０６）。不一致であれば否認を連絡する（ステップ１１０７）。なお、図４のシステムも同様の処理である。

【００４４】図１２は、図４のシステムにおける個人の管理用鍵４１８の生成と登録の流れ、すなわち公開鍵ペア４１８の公開鍵を鍵管理サーバ４０３に鍵４２３として登録する場合のフローチャートを示したものである。ステップ１２０２，１２０３は図５のステップ５０２，５０３と同様の処理である。図５との相違は、個人管理用鍵の生成が必ず公開鍵ペア（公開鍵と秘密鍵）であること（ステップ１２０２）、及び個人管理用公開鍵ペア４１８のうち公開鍵を鍵管理サーバに鍵４２３として登録する（ステップ１２０４）ことである。

【００４５】図１３は、図４のシステムの個人クライアント４０２における取引の実行のフローチャートを示したものである。ステップ１３０４～１３０６は図７のステップ７０３～７０５と同様の処理である。図７との相違は、取引を開始する前に個人管理用公開鍵ペア４１８の秘密鍵で個人証明書に署名し、鍵管理サーバ４０３に送付することである（ステップ１３０２）。鍵管理サーバから個人認証ＯＫで返ってくれば（ステップ１３０３）、以降は図７と同様である。個人認証ＮＧであれば、取引き処理はできない。

【００４６】図１４は、図４のシステムの鍵管理サーバ４０３での個人認証のフローチャートを示したものである。鍵管理サーバ４０３の個人認証処理が開始されると（ステップ１４０１）、個人クライアント４０２から図１３で示したように個人証明書を受け付け（ステップ１４０２）、鍵管理サーバ４０３に登録されている鍵管理用公開鍵４２３を使用して、送付された個人証明書の署名を検証する（ステップ１４０３）。検証ＯＫであれば、個人認証ＯＫを個人クライアント４０２に返信し（ステップ１４０５）、当該個人ＩＤからの取引用公開鍵取得要求を許可状態にする（ステップ１４０６）。検証ＮＧであれば、個人認証の否認を個人クライアント４０２に返信し（ステップ１４０７）、当該個人ＩＤからの取引用公開鍵取得要求を不許可状態にする（ステップ１４０８）。図１５は、鍵インデックスに許可、不許可状態を示すフラグ１５０８を持つ場合の例である。

【００４７】図１５は、鍵管理サーバに持つ鍵インデクスの例である。この鍵インデクスは、取引用公開鍵ペアを識別する鍵ＩＤ１５０１、所有者を識別する個人ＩＤ

１５０２、取引先のアプリケーションサーバを識別する取引先ＩＤ１５０３、鍵の累積の使用回数を示すカウンタ１５０４、１日の使用回数を示すカウンタ１５０５、１週間の使用回数を示すカウンタ１５０６、１ヶ月の使用回数を示すカウンタ１５０７、この鍵の使用が許可されているか否かの状態を示す状態フラグ１５０８、最後に使用した日時を示す領域１５０９、鍵の有効期限を示す設定領域１５１０、累積の使用回数限度を示す設定領域１５１１、１日の使用回数限度を示す設定領域１５１２、１週間の使用回数限度を示す設定領域１５１３、及び１ヶ月の使用回数限度を示す設定領域１５１４などからなる。

【００４８】図１６は、取引先インデクスの例である。取引先インデクスは、取引先のアプリケーションサーバを識別するための取引先ＩＤ１６０１，取引先の名称１６０２、アプリケーションサーバの名称１６０３、及び業務内容１６０４などからなる。図１の例では取引先インデクスを個人クライアントに持つため、同一のアプリケーションサーバであっても取引先ＩＤは個人毎にばらばらである。図２、図３、図４では鍵管理サーバで管理するため、同一のアプリケーションサーバの取引先ＩＤは同一である。

【００４９】図１７は、鍵管理サーバで持つ管理用の鍵インデクスの例である。管理用の鍵インデクスは、管理用鍵の識別をするための個人管理用鍵ＩＤ１７０１、所有者を識別するための個人ＩＤ１７０２、及び暗号種別などの管理用鍵の付加情報を示す管理用鍵情報１７０３からなる。

【００５０】なお、上記実施形態ではネットワーク経由の安全な取引を行う場合を想定しており、基礎技術として公開鍵暗号技術を想定している。公開鍵暗号は秘密鍵と公開鍵の２つの鍵をペアで使用する暗号技術であり、秘密鍵を他者に知られることなく管理することで安全が維持されている。公開鍵暗号技術に関連して公開鍵と秘密鍵を保持している者を認証するために認証局を使用する方式も普及している。この場合、公開鍵に対応して電子認証書を認証局が発行し、取引時には秘密鍵・公開鍵に加え、電子認証書を使用することでさらに安全が高まる。本発明は、電子認証書も公開鍵と組み合わせて管理することに容易に拡張することができる。

【００５１】

【発明の効果】以上説明したように、本発明によれば、各クライアントは１個の鍵管理用鍵を管理するだけで、セキュリティを確保しながらアプリケーションサーバごとの取引用鍵を扱うことができる。したがって、各クライアントでの鍵管理は容易であり、携帯端末からの取引も容易に行える。また、鍵管理サーバで、鍵使用条件の検証、取引用鍵の検証、及び公開鍵技術を使用した個人の認証も可能である。

【図面の簡単な説明】

【図１】本発明の第１の実施形態のシステムの構成図である。

【図２】本発明の第２の実施形態のシステムの構成図である。

【図３】本発明の第３の実施形態のシステムの構成図である。

【図４】本発明の第４の実施形態のシステムの構成図である。

【図５】個人クライアントにおける個人の管理用鍵生成のフローチャート図である。

【図６】個人クライアントにおける取引用鍵の生成と登録のフローチャート図である。

【図７】個人クライアントにおける取引の実行のフローチャート図である。

【図８】鍵管理サーバにおける条件検証（有効期限の通知）のフローチャート図である。

【図９】鍵管理サーバにおける条件検証（使用回数限度の通知）のフローチャート図である。

【図１０】個人クライアントにおける取引用鍵の生成と登録のフローチャート図である。

【図１１】鍵管理サーバにおける取引用公開鍵の認証のフローチャート図である。

【図１２】個人クライアントにおける個人の管理用公開鍵の生成と鍵管理サーバへの登録のフローチャート図である。

【図１３】取引用公開鍵ペア取得のための個人認証後、取引の実行を行う場合のフローチャート図である。

【図１４】鍵管理サーバでの個人認証処理のフローチャート図である。

【図１５】取引用鍵インデクスの形式を示す図である。

【図１６】取引先インデクスの形式を示す図である。

【図１７】個人の管理用公開鍵のインデクスの形式を示す図である。

【符号の説明】

１０１…個人

１０２…個人クライアント

１０３…鍵管理サーバ

１０４…鍵管理サーバの鍵格納領域

１０５…個人取引用公開鍵ペア１（公開鍵と秘密鍵伴に暗号化）

１０６…個人取引用公開鍵ペア２（公開鍵と秘密鍵伴に暗号化）

１０７…取引用鍵インデクス

１０８…鍵管理サーバの鍵登録部（個人取引用公開鍵ペア）

１０９…鍵管理サーバの条件検証部（有効期限、使用回数限度）

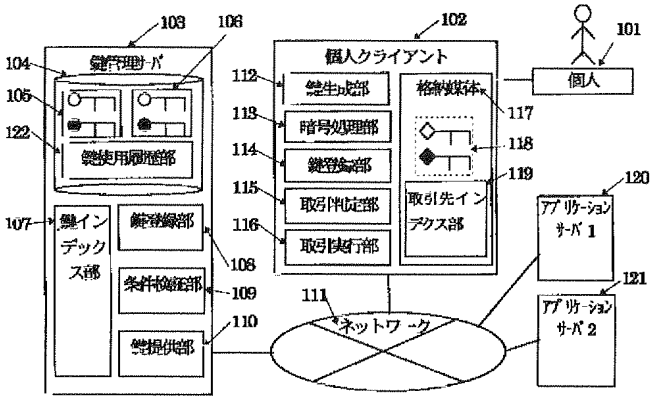
１１０…鍵管理サーバの鍵提供部

１１１…ネットワーク

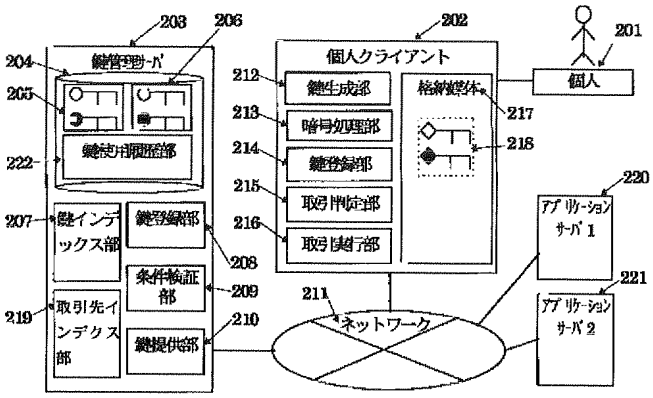
１１２…個人クライアントの鍵生成部

１１３…個人クライアントの暗号処理部
１１４…個人クライアントの鍵登録部
１１５…個人クライアントの取引判定部
１１６…個人クライアントの取引実行部
１１７…格納媒体
１１８…個人クライアントの個人鍵管理用鍵
１１９…個人クライアントの取引先インデクス
１２０…アプリケーションサーバ１
１２１…アプリケーションサーバ２
１２２…鍵使用履歴部
２０１…個人
２０２…個人クライアント
２０３…鍵管理サーバ
２０４…鍵管理サーバの鍵格納領域
２０５…個人取引用公開鍵ペア１（公開鍵と秘密鍵伴に暗号化）
２０６…個人取引用公開鍵ペア２（公開鍵と秘密鍵伴に暗号化）
２０７…取引用鍵インデクス
２０８…鍵管理サーバの鍵登録部（個人取引用公開鍵ペア）
２０９…鍵管理サーバの条件検証部（有効期限、使用回数限度）
２１０…鍵管理サーバの鍵提供部
２１１…ネットワーク
２１２…個人クライアントの鍵生成部
２１３…個人クライアントの暗号処理部
２１４…個人クライアントの鍵登録部
２１５…個人クライアントの取引判定部
２１６…個人クライアントの取引実行部
２１７…格納媒体
２１８…個人クライアントの個人鍵管理用鍵
２１９…鍵管理サーバ内の取引先インデクス
２２０…アプリケーションサーバ１
２２１…アプリケーションサーバ２
２２２…鍵使用履歴部
３０１…個人
３０２…個人クライアント
３０３…鍵管理サーバ
３０４…鍵管理サーバの鍵格納領域
３０５…個人取引用公開鍵ペア１（秘密鍵のみ暗号化）
３０６…個人取引用公開鍵ペア２（秘密鍵のみ暗号化）
３０７…取引用鍵インデクス
３０８…鍵管理サーバの鍵登録部（個人取引用公開鍵ペア）
３０９…鍵管理サーバの条件検証部（有効期限、使用回数限度）
３１０…鍵管理サーバの鍵提供部
３１１…ネットワーク
３１２…個人クライアントの鍵生成部
３１３…個人クライアントの暗号処理部
３１４…個人クライアントの鍵登録部
３１５…個人クライアントの取引判定部
３１６…個人クライアントの取引実行部
３１７…格納媒体
３１８…個人クライアントの個人鍵管理用鍵
３１９…鍵管理サーバ内の取引先インデクス
３２０…アプリケーションサーバ１
３２１…アプリケーションサーバ２
３２２…鍵管理サーバの個人公開鍵認証部
３２３…鍵使用履歴部
４０１…個人
４０２…個人クライアント
４０３…鍵管理サーバ
４０４…鍵管理サーバの鍵格納領域
４０５…個人取引用公開鍵ペア１（秘密鍵のみ暗号化）
４０６…個人取引用公開鍵ペア２（秘密鍵のみ暗号化）
４０７…取引用鍵インデクス
４０８…鍵管理サーバの鍵登録部（個人取引用公開鍵ペア）
４０９…鍵管理サーバの条件検証部（有効期限、使用回数限度）
４１０…鍵管理サーバの鍵提供部
４１１…ネットワーク
４１２…個人クライアントの鍵生成部
４１３…個人クライアントの暗号処理部
４１４…個人クライアントの鍵登録部
４１５…個人クライアントの取引判定部
４１６…個人クライアントの取引実行部
４１７…格納媒体
４１８…個人クライアントの個人鍵管理用公開鍵ペア
４１９…鍵管理サーバ内の取引先インデクス
４２０…アプリケーションサーバ１
４２１…アプリケーションサーバ２
４２２…鍵管理サーバの個人公開鍵認証部
４２３…個人鍵管理用公開鍵ペアの公開鍵
４２４…個人鍵管理用公開鍵のインデクス
４２５…個人クライアントの署名生成部
４２６…鍵管理サーバの個人認証部
４２７…鍵使用履歴部

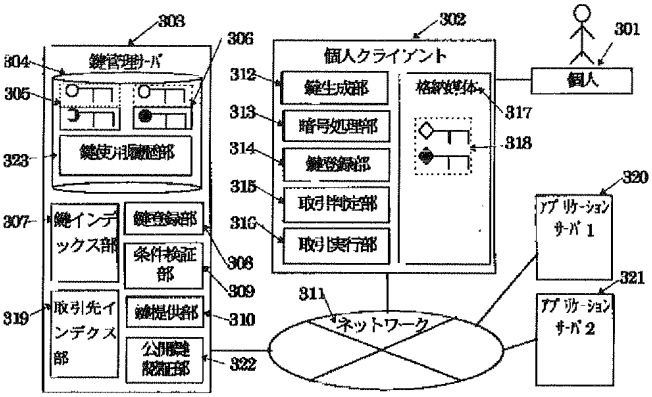
【図１】



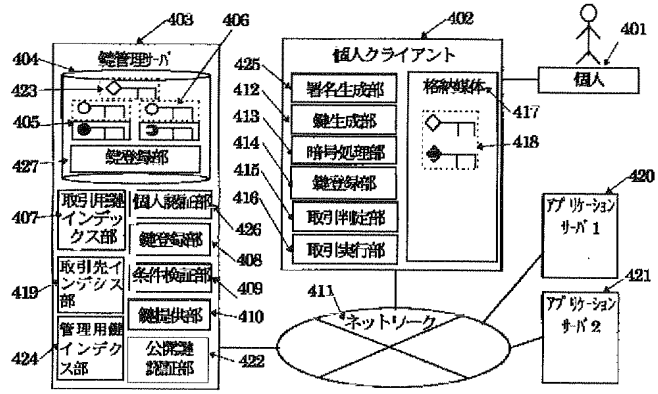
【図２】



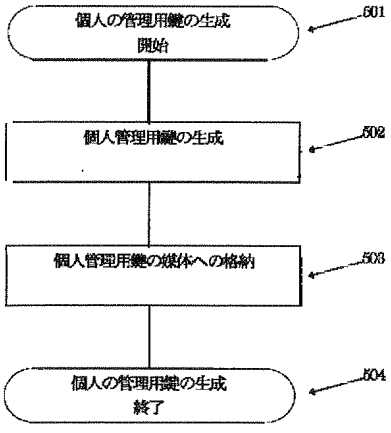
【図３】



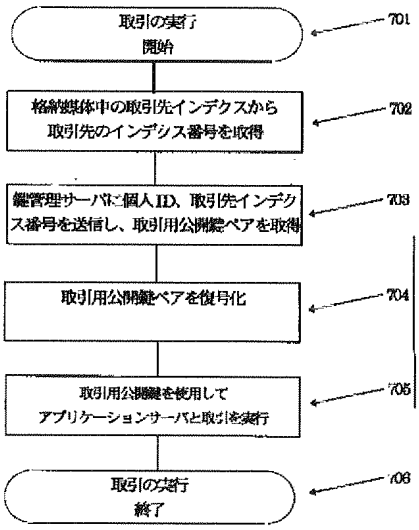
【図４】



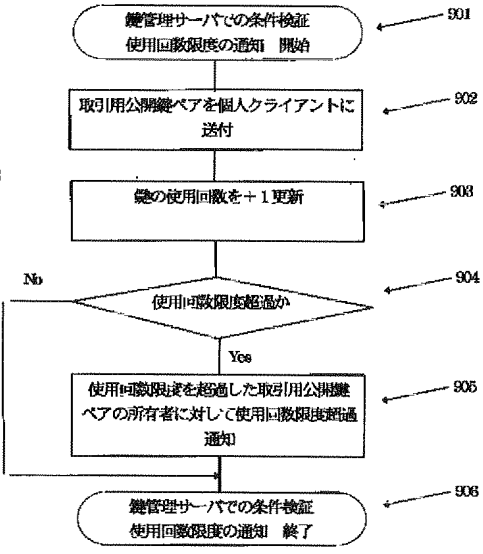
【図５】



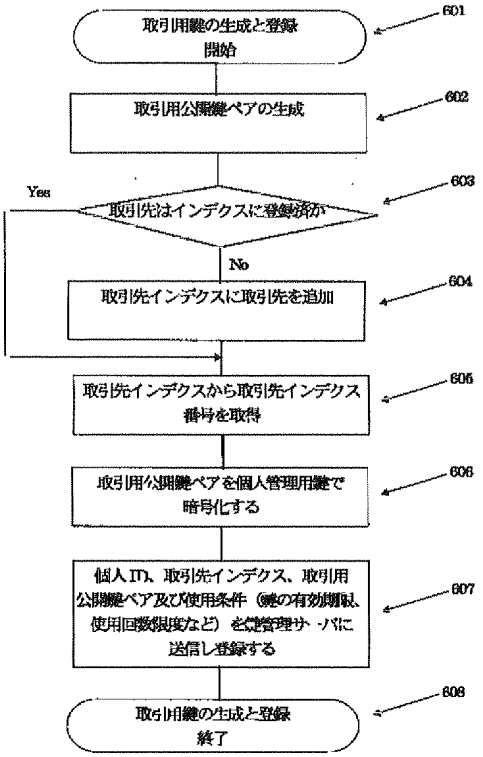
【図７】



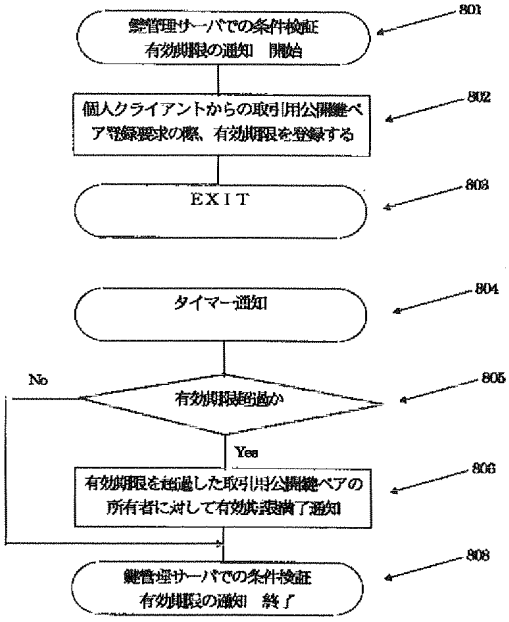
【図９】



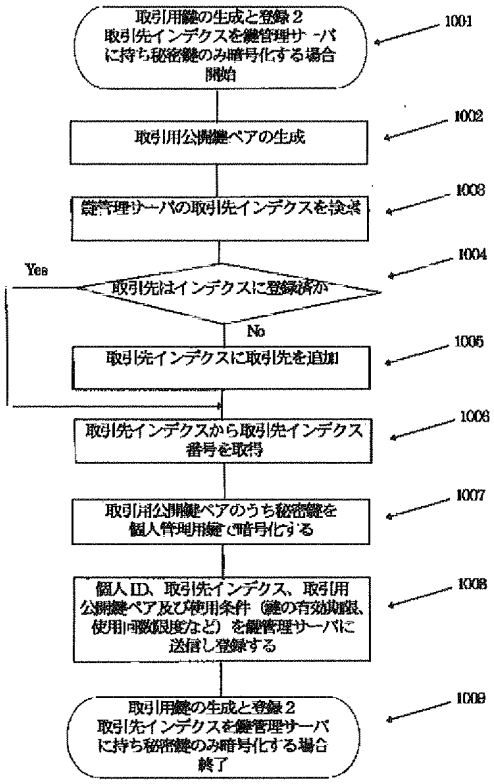
【図６】



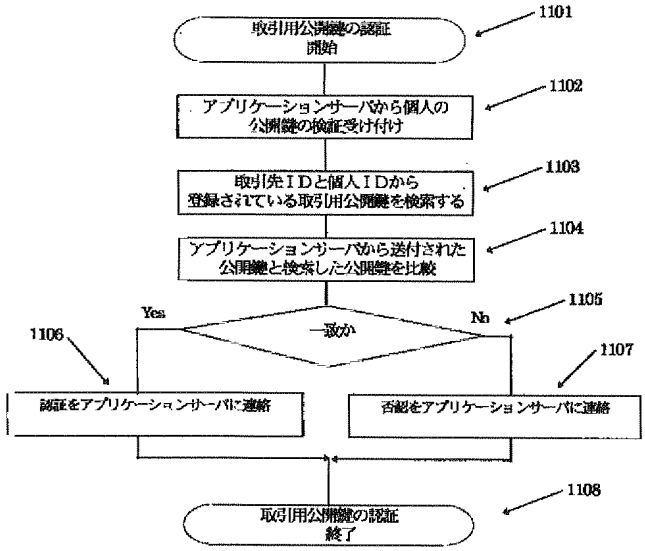
【図８】



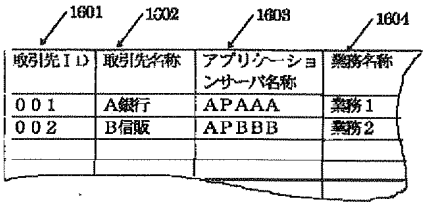
【図１０】



【図１１】

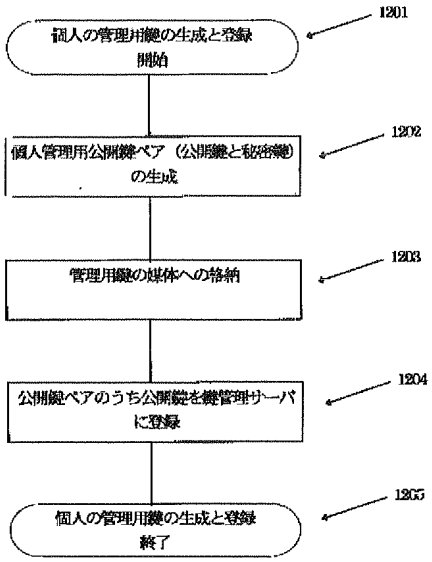


【図１６】

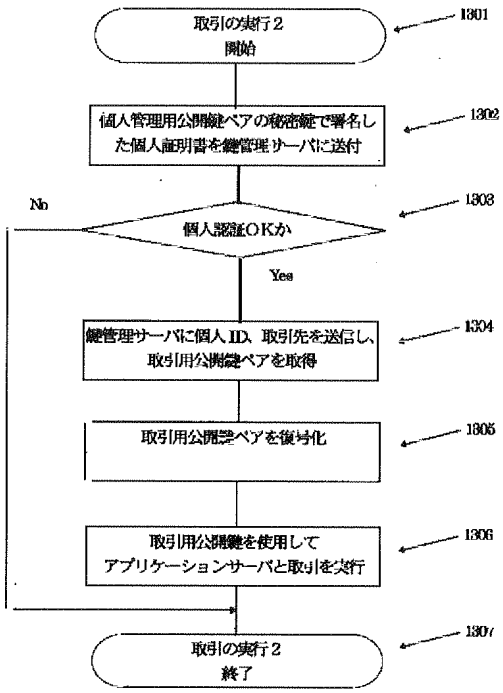


1601 取引先ＩＤ	1602 取引先名称	1603 アプリケーションサーバ名称	1604 業務名称
００１	A銀行	APAAA	業務１
００２	B信販	APBBB	業務２

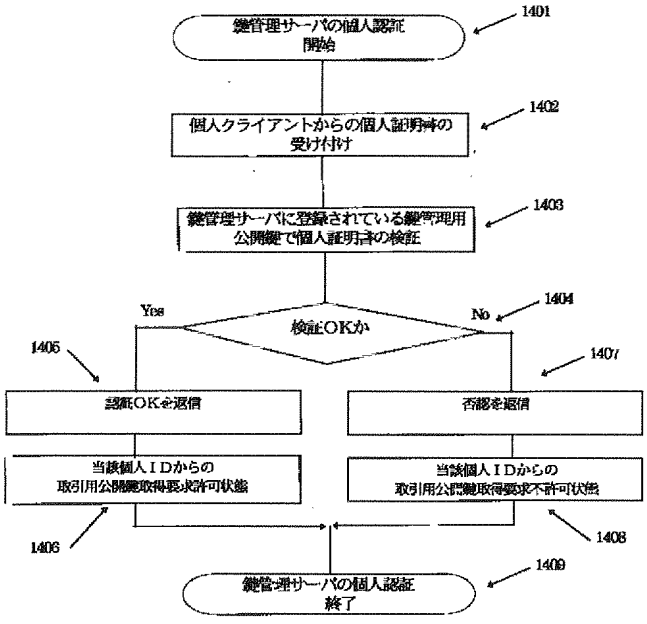
【図１２】



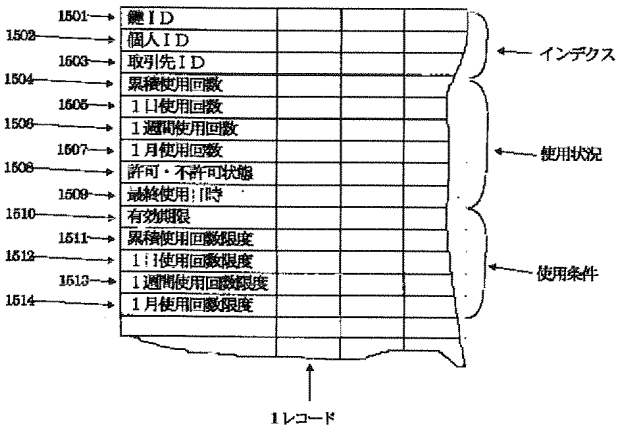
【図１３】



【図１４】



【図１５】



【図１７】